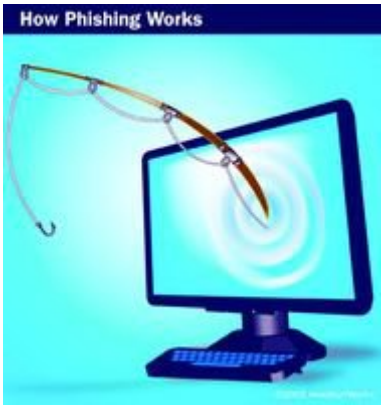
Phishing for Information

by Sandra Isnaji

For the online version go to http://www.thesundaily.com/article.cfm?id=43200

I'm a nobody.
Who wants to steal my online identity, anyway?



I use yahoomail account for social networking purposes and I have unchecked all email notification from Facebook.

So, I was surprised to see an email from the social networking site which was sent to my company email address. Strangely, the email was addressed to my colleague and yet it sat there on my mailbox.

Looking at it, I recognised the basic telltales of a phishing email. Social networking sites or banks will never ask customers to update account information via email links.

Other than that, phishing link usually have typo error such as: www.facebjokokn.com/login/index.html, instead of www.facebook.com; or extra words such as www.verify-microsoft.com, instead of www.microsoft.com

It was the first time I received a phishing email that was supposed to have originated from a social networking site. For research purpose, I clicked on the phishing link (please don't do this at home!), and found myself staring at a page that looks exactly like the real Facebook login page.

Definitely a phishing scam – which is a type of deception designed to fish for valuable personal data, such as bank accounts details, credit card numbers, Windows Live IDs, social networking account data, or other information.

Phishing is also known as identity theft. Scammers or phishers have been known to utilise various methods of social engineering such as persuasion, flirting, and blackmail/threat, usually with financial gain in mind.

Over the last 10 years or so of my Internet life, I've received many kinds of phishing emails similar to the example cited above. Some of the common ones: schools/colleges offering instant degrees; someone inheriting so much money that he needed to split the money with a total stranger; some banks that you had never dealt with but strangely asking you to verify your account details; and so-called employment agencies offering opportunities to earn lots of money.

Most of the emails are easy enough to ignore as they are either too suspicious or too good to be true. But in 2001, I totally fell for a phishing email purportedly sent by an anti-virus company.

The email said that a vulnerability was detected in my computer, and I had to quickly click on the link given to solve the problem. How kind, I thought. Naive, and paranoid of virus attack, I followed all the instructions given. Not long after that, my hard disk crashed.

A few months later, I received a similar email, and like an idiot I repeated my mistake, and of course my hard disk crashed again.

I didn't know it was the phishing email that caused my computer to crash, until I became educated on phishing and malware issues some six to seven years later.

So the next time your hard disk crash for seemingly no reason at all, do stop and think about it. You've probably received a phishing email and in a brief moment of doubt, you absent-mindedly clicked, thus giving a malware like the infamous Conficker, for example, a chance to get installed in your computer without you realising it.

Other than emails, text messages or SMS are also used for phishing.

Some time in 2006, I received a text message saying I won RM9,000 purportedly from a popular reality talent show contest organised by a major broadcasting company based in Kuala Lumpur. I suspected it was a scam because I didn't remember taking part in such a contest. Out of curiosity, I called, and a man with a foreign accent answered. He confirmed that I won, and asked for my credit card details in order to give me my cash prize.

I refused.

I told him I lived in Kuala Lumpur and would personally collect the prize, but he insisted that winners are not allowed to do so. Then he asked for my savings account number and even my ATM card's personal identification number (PIN). I told him I didn't have any bank account at all. He didn't believe me and we argued until he gave up on me.

I happen to know someone who lost his one-month salary to a phishing scammer but was too embarrassed to report the incident. He remembered being dazzled by the promise of a huge winning and recounted how, as if under a spell, he gave away his ATM card number and PIN.

Only when the cash prize never seemed to get credited into his bank account, and when his salary went missing from that bank account, did he realise he had been duped.

Now you may be wondering why the phishing scammers are interested in stealing other people's social networking username and passwords.

But think about it. I mean the criminal could sign-in to my Facebook, pretend to be me (who is supposed to be in some kind of financial trouble), send messages direct to the inboxes of all my 'Facebook friends' asking them to bank in cash urgently to a given account number in order to rescue me (with a solemn promise to pay them back).

Of course, all that money will go into the phisher's bank account, while my friends will be coming after me.

With the rapidly increasing number of Internet users in Malaysia – now hovering at around 16 to 17 million – it is easy to see why criminals are targeting Malaysians. To avoid becoming a victim of phishing, we must always be vigilant.

Remember what our parents used to say: "Don't talk to strangers." The same principle applies in cyber world: "Don't entertain email/sms from strangers!"

To learn more, visit Anti-Phishing Working Group (APWG) at www.antiphishing.org, or get tips from www.cybersafe.my
Report phishing scams to cyber999@cybersecurity.my